MONTHLY TECHNICAL REPORT

DoD PKI MIGRATION TO OPEN STANDARDS

September 30, 1999

Prepared By:

Defense Information Systems Agency
JIEO Center For Information Technology Standards

TABLE OF CONTENTS

1. OVERVIEW

This technical report contains an August/September 1999 summary of ongoing analyses performed on PKI-related products for conformance to standards, and to evaluate the PKI standards themselves for suitability to DoD requirements. This work is being conducted in the Standards Analysis Facility (SAF) at Ft. Monmouth, NJ by the Network Applications and Security Branch of the DISA Center For Information Technology Standards (CFITS). The SAF supports testing of the DoD PKI server environment to related commercial vendor products including:

- Netscape End-Entity (EE) applications;
- Microsoft (MS) EE applications;
- Lotus EE applications;
- MS PKI-enabled Server applications;
- Lotus PKI-enabled Server applications;
- Internet PKIX Reference Implementation (Jonah);
- Federal PKI MISPC Reference Implementation;
- LDAP vendor products;
- S/MIME vendor products.

2. DOD PKI STANDARDS EVALUATIONS

2.1 BACKGROUND

The SAF has set up within a DoD PKI Test Environment in order to support the current DoD PKI implementation. This support consists of evaluating the developing suite of PKI standards generated by: the Internet Engineering Task Force (IETF); the Federal Government; the DoD; and ancillary standard groups. Closely related to this work is: evaluating the most widely used vendor products that are being used in DoD networks; examining PKI capabilities of new software that will eventually be introduced into the DoD network; and determining how well the DoD PKI implementation conforms to the required standards.

The DoD PKI Test Environment is a mirror of the technology used in the Pilot DoD PKI consisting of: a Root Certificate Authority (CA); two each intermediate Identify (ID) and E-mail CAs; associated Directory Servers (DSs); multiple web servers; a Domain Name Service (DNS) server; POP3 and IMAP mail servers; and multiple client machines. The client machines are all MS Windows NT-based and either has MS Windows NT 4 Server with Service Pack 4 or MS Windows NT 5 (Beta) Server loaded. The server machines are UNIX-based Sun Workstations with the Common Operating Environment (COE) as a foundation loaded with an image of the currently fielded Pilot DoD PKI software.

2.2 ANALYSIS

This month's PKI standards analysis focused on the following areas:

- Microsoft CA/DS capabilities analysis;
- Lotus CA/DS capabilities analysis;
- Status and Analysis of standards conformance tables against the NIST and Jonah Reference Implementations;
- S/MIME standards and associated commercial products.

2.3 MICROSOFT CA/DS CAPABILITIES ANALYSIS

Microsoft (MS) Windows 2000 RC1 Build 2072 Beta3was obtained and loaded onto a SAF PC for the purpose of evaluating MS's Certificate Authority and Directory Service capabilities, in particular, conformance to the IETF PKIX standards, Fed TWG initiatives, and the DoD PKI.

To date, the MS CA has been successfully brought online as a standalone CA. The CA is able to issue Certificates and also certify itself. An initial analysis of the implementation was performed using the DoD PKI Functional Specification compliance table. The results of this run is included in Appendix B. Generally speaking, the results of the partial evaluation indicate that the MS product is very much in compliance with the Netscape-based implementation being used within the current DoD PKI.

However, it has been discovered that an email sent from Outlook to Netscape causes Netscape to crash. This occurs when a cert is created using the Windows 2000 Certificate Server. The email that causes the crash is a signed email sent to Netscape Messenger. Setting the CA2000 CA to a trusted certificate authority within Netscape does not prevent Netscape from crashing. Before Netscape crashes it is able to download and insert the MS CA certificate into its database of Certificate Signers. The user then manually goes into the Netscape security database and approves the CA2000 certificate authority. (This same signed email does not cause Outlook to crash when reading it). A possible cause of the problem is CA2000 has extensions that Netscape does not expect. Further investigation is ongoing.

Products evaluated include:

- Microsoft Windows 2000 Server Build 2072 Certificate Server (aka CA2000)
- Outlook Express 5 on Windows 2000
- Outlook Express 5 on NT4
- Outlook Express 4
- Netscape Messenger V4.61 on NT4
- Netscape Messenger V4.51 on NT4
- Netscape Messenger V4.04 on NT4.

2.4 LOTUS VERSION 5 CA/DS CAPABILITIES ANALYSIS

A copy of Domino/Notes Version 5 was obtained for evaluation of standards conformance. Generally speaking, the Lotus software products are extremely difficult to install, configure, and operate. This problem is due in part to very limited documentation included with the product. Their online documentation is also very limited, and the product line is not as intuitive as is other network software products.

The Domino server product is being installed with the assistance of DISA Ft. Monmouth Network Operations staff, two highly experienced technical people, who despite their experience are having trouble properly configuring the Version 5 system. One problem in particular that had plagued them involved setting up the system administrator profile correctly, a problem that apparently is well known to users of the product based on their postings online. This problem has been overcome and configuration of the various servers is continuing, along with loading an upgrade version that was obtained recently through licensing agreement.

Lotus Notes 5.0 did not have the capability to import certs generated by other vendor products, including Netscape. Version 5.01 was obtained which allows this capability. A cert generated by the Netscape-based DoD PKI implementation was successfully imported into the Notes 5.01. Also a cert was imported into Microsoft Outlook. Signed and encrypted mail was successfully exchanged between Netscape Navigator, Microsoft Outlook, and Lotus Notes.

2.5 EVALUATIONS OF THE NIST RI AND JONAH RI

Both the NIST and Jonah Reference Implementations (RIs) were evaluated for conformance to both the DoD PKI and PKIX conformance tables. Results were less than favorable due to the fact that both of these products are not full-blown PKI implementations and limited in functionality. The results of the table(s) analysis indicates that neither of these products (in current form) are capable of acting as a formal reference implementation that would meet DoD needs.

Summary of NIST RI Evaluation:

- Both the DoD PKI Functional Specification Table and the PKIX-compliant package of Tables were run against NIST V1;
- Inter-process communications are handled via email instead of SSL;
- Some of the more important extensions are not yet enabled (e.g.; Key Usage);
- No configuration capabilities to create specialized certificates such as email;
- Installation instructions were very explicit and thorough resulting in an easy installation of the CA product;
- Instructions on interoperable directory products was vague, resulting in a significant amount of time being lost trying to configure Netscape Directory Version 4. Only Netscape Version 3 will work properly.
- Results of the compliance table analyzes are included as Appendix C.

Summary of the Jonah RI Evaluation:

- Only the DoD PKI Functional Specification Table was run against the Jonah RI;
- SSL communications is not supported;
- As configured, it appears only Version 1 Certs are supported;
- RSA is not implemented;
- Some of the Key Usage extensions are not supported yet (such as Key Encipherment);
- The parent groups responsible for its development (IBM, Lotus, Iris, Cylink) have made the decision to no longer support the freeware version, instead proceeding with development of a commercial version.
- For the last reason mainly, it was decided to drop Jonah from any further research and use.

2.6 S/MIME STANDARDS ANALYSIS

Work has just started in this area. The focus is on evaluating the emerging S/MIMEv3 standards for fit to DoD requirements for secure mail. The research will be based on the IETF standards defining S/MIME V3 including but not limited to: S/MIMEv3 Cryptographic Message Syntax (RFC 2630), S/MIMEv3 Certificate Handling (RFC 2632), S/MIMEv3 Messaging (RFC 2633), and the draft Certificate Distribution Specification. Efforts to date include the development of conformance tables for these four protocols and the acquisition of a S/MIMEv3 Reference Implementation obtained from J G Van Dyke, which is currently being loaded within the SAF. Van Dyke developed the RI for NSA use. The code must be compiled before use and has been successfully compiled within the SAF. Status at this point is determining the capabilities and user interface of the executable software in order to determine an evaluation plan.

APPENDIX A: GLOSSARY

a.k.a.	Also Known As
CA	Certificate Authority
CFITS	Center for Information Technology Standards
COE	Common Operating Environment
COTS	Commercial off the Shelf
DDK	MS Driver Developers Kit
DER	Distinguished Encoding Rules
DII	Defense Information Infrastructure
DNS	Domain Name Server
DS	Directory Server
IE4	Microsoft Internet Explorer 4.01
IE5	Microsoft Internet Explorer 5 (BETA)
IETF	Internet Engineering Task Force
IP	Internet Protocol
SAF	Standards Analysis Facility (DISA Ft. Monmouth, NJ)
LDAP	Lightweight Directory Access Protocol
MMC	Microsoft Management Console
NT4	Microsoft NT 4
NT5	Microsoft NT 5 (BETA)
.p7c	Cryptographic Message Syntax Standard – PKCS#7
PC	Personal Computer
.pfx/.p12	Personal Information Exchange – PKCS#12
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
POP3	Post Office Protocol 3
RA	Registration Authority
RAM	Random Access Memory
Sigverif	Signature Verification Utility
SP4	Service Pack 4 (Microsoft released Nov 98)

APPENDIX B – Microsoft Analysis

Product under Evaluation:

Microsoft Certificate Authority (standalone, Windows 2000 RCI, Build #2072, Beta 3)

Evaluated for compliance to with the DOD Medium Assurance PKI Functional Specification, v0.3, 20 OCT 98.

Compliance codes: Y - System supports requirements
N - System does not support requirement
P - System partial supports requirement
A - Analysis pending

Requirement	Reference	Comply	Comment
General		CA | EE	
Configurable Parameters	3.1.1	Y | Y	
SSL	3.1.2	Y | Y	SSL Certs are V3, but need to
Confidential Administrative Communications	3.1.3	A | A	Configure CA to use SSL thru IIS server
Certificate Fields		CA | EE	
Version	3.2.1.1	Y | Y	Version 3
Serial Number	3.2.1.2	Y | Y	Certs are numbered sequentially
Signature	3.2.1.3	Y | Y	RSA 1024 for CA/EE (512-4096)
Issuer	3.2.1.4	Y | Y	DN = CN, OU…, O, C
Validity	3.2.1.5	Y | Y	Setable, default is 2 years
Subject	3.2.1.6	Y | Y	
Subject Public Key Information	3.2.1.7	Y | Y	RSA
Issuer Unique Identifier not used	3.2.1.8	Y | Y	Not Used
Subject Unique Identifier not used	3.2.1.9	Y | Y	Not used
Issuer's Signature	3.2.1.11	Y | Y	SHA1 w/RSA
Certificate Extensions		CA | EE	
Authority Key Identifier	3.2.2.1.1	Na | Y	Key ID, CA DN, Cert Serial #
Subject Key Identifier	3.2.2.1.2	Y | na	Unique #
Key Usage: Digital Signature	3.2.2.1.3	Y | Y	
KU: Non-repudiation	3.2.2.1.3	Y | Y	

Requirement	Reference	Comply	Comment
KU: Key Encipherment	3.2.2.1.3	na | Y	
KU: Certificate Signing	3.2.2.1.3	Y | na	
KU: CRL Signature	3.2.2.1.3	Y | na	Also KU for “off-line CRL signing”
Private Key Usage Period not used	3.2.2.1.4	Y | Y	Not used
Certificate Policies	3.2.2.1.5	N | N	
Policy Mapping not used	3.2.2.1.6	Y | Y	Not used
Subject Alternative Names	3.2.2.2.1	Na | A	This may be setable in policy module
Issuer Alternative Names	3.2.2.2.1	Na | Y	
Subject Directory Attributes not used	3.2.2.2.2	Y | Y	Not Used
Basic Constraints	3.2.2.3	Y | N	
Name Constraints	3.2.2.3	N | N	
Policy Constraints	3.2.2.3	N | N	
CRL Distribution Points	3.2.2.4.1	Y | Y	
Signing Algorithms		CA | EE	
RSA	3.2.3.1	Y | Y	Default uses RSA
DSS	3.2.3.2	A | A	Available, not determined how to set properly
Certificate Types		CA | EE	
Root CA	3.2.4.1.1	Y | na	
Signing CA	3.2.4.1.2	Y | na	
Identity	3.2.4.2.1	Na | Y	
E-mail	3.2.4.2.2	Na | Y	
Server	3.2.4.2.3	Na | Y	
Developer (code signing)	3.2.4.2.4	Na | Y	
Enabled Device	3.2.4.2.5	Na | Y	
Certificate Revocation List (CRL) Fields		CA | EE	
Version	3.3.1.1	Y | na	Version 2 CRLs
Issuer Name	3.3.1.2	Y | na	
This Update	3.3.1.3	Y | na	
Next Update	3.3.1.4	Y | na	
Revoked Certificates	3.3.1.5	Y | na	
CRL Extensions		CA | EE	
Authority Key Identifier	3.3.2.1	Y | na	
Issuer Alternative Name not used	3.3.2.2	Y | na	
CRL Number	3.3.2.3	N | na	Date stamp included
Issuing Distribution Point	3.3.2.4	N | na	Cert has CRL Distribution points
Delta CRL Indicator	3.3.2.5	N | na	Optional
CRL Entry Extensions		CA | EE	

Requirement	Reference	Comply	Comment
Reason Code: Unspecified not used	3.3.3.1	P | na	Available option, not required
RC: Key Compromise	3.3.3.1	Y | na	When revoking asks for reason code
RC: CA Compromise	3.3.3.1	Y | na	
RC: Affiliation Changed	3.3.3.1	Y | na	
RC: Superseded	3.3.3.1	Y | na	
RC: Cessation of Operations	3.3.3.1	Y | na	
RC: Certificate Hold not used	3.3.3.1	Y | na	
RC: Remove from CRL	3.3.3.1	N | na	Not available
Expiration Date not used	3.3.3.2	Y | na	
Instruction Code	3.3.3.3	Y | na	
Invalidity Date	3.3.3.4	N | na	Not used in DoD PKI
Certificate Issuer	3.3.3.5	N | na	" "
Directory Schema		CA | EE	
Directory Hierarchy	3.4.1	Y | na	
Distinguished Names	3.4.2	Y | na	
CA Directory Objects	3.4.3.1	Y | na	
Individual Directory Objects	3.4.3.2	Y | na	
Country Object	3.4.3.3	Y | na	
Organization Objects	3.4.3.4	Y | na	
Organizational Unit Objects	3.4.3.5	Y | na	
PKI Roles Objects	3.4.3.6	Y | na	
Device Objects	3.4.3.7	A | na	Further analysis required
Processes		CA | EE	
Identification, Authentication and Access Control of CA Personnel	3.5.1.1	Y | na | |	
Identification, Authentication and Access Control of RA Personnel	3.5.1.2	P | na	The RA/LRA roles are not pre-packaged w CA/2000. May be programmed.
Identification, Authentication and Access Control of LRA Personnel	3.5.1.3	P | na	" "
Identification, Authentication and Access Control of Subscribers	3.5.1.4	Y | Y	
Identity Certificate	3.5.2.1	Y | Y	

Requirement	Reference	Comply	Comment
Authorization, Request and Issue			
Email Certificate Authorization, Request and Issue	3.5.2.2	Y | Y	
Other Certificate Authorization, Request and Issue	3.5.2.3	Y | na	Other cert types may be created by entering new OID
Disabling Pre-Authorizations	3.5.2.4	Y | na	
Processing Authorizations	3.5.2.5	Y | na	
Certificate Renewal and Reissue	3.5.3	Y | na	Windows 2000 will automatically request new certs (updates) and manage old certs
Certificate Expiration	3.5.4	Y | na	
Certificate Revocation	3.5.5	Y | na	An easy interface is provided
CRL Management	3.5.6	Y | na	CRLs may be issued out of cycle
Certificate Removal	3.5.7	Y | na	
Key Generation	3.5.7.1	Y | na	
Key Recovery and Key Protection	3.5.8	Y | na	
System Configuration	3.5.9.1	Y | na	
CA Management	3.5.9.2	Y | na	
Key Management	3.5.9.3	Y | na	
User Role Management	3.5.9.4	Y | na	
System Administrator	3.5.9.5	Y | na	
CA Staff	3.5.9.6	Y | na	
RA	3.5.9.7	P | na	CA admin rights may be given to other users. RA/LRA function would have to be created
LRA	3.5.9.8	P | na	“ “
Audit Logs	3.5.10	Y | na	
Archive	3.5.11	Y | na	
Interfaces		CA | EE	
User Web Interface for Certificate Request	3.6.1.1.1		
User Web Interface for Certificate Issue	3.6.1.1.2		
User Web Interface for Directory Search	3.6.1.1.3		
System Administrator Interface	3.6.2.1		

Requirement	Reference	Comply	Comment
CA Staff Interface	3.6.2.2		
RA Interface	3.6.2.3		
LRA Interface	3.6.2.4		

APPENDIX C – NIST MISPC Analysis

Product under Evaluation:

NIST MISPC Reference Implementation Version 1.0

for compliance to the DOD Medium Assurance PKI Functional Specification, v0.3, 20 OCT 98.

Compliance codes: Y - System supports requirements
N - System does not support requirement
P - System partial supports requirement
A - Analysis pending

Requirement	Reference	Comply	Comment
General		CA | EE	
Configurable Parameters	3.1.1	P | P	Only the cert policy criticality may be set
SSL	3.1.2	N | N	Process user email, not SSL
Confidential Administrative Communications	3.1.3	P | P	Emails are signed, but not encrypted
Certificate Fields		CA | EE	
Version	3.2.1.1	Y | Y	
Serial Number	3.2.1.2	Y | Y	
Signature	3.2.1.3	Y | Y	
Issuer	3.2.1.4	Y | Y	
Validity	3.2.1.5	Y | Y	
Subject	3.2.1.6	Y | Y	
Subject Public Key Information	3.2.1.7	Y | Y	
Issuer Unique Identifier not used	3.2.1.8	Y | Y	
Subject Unique Identifier not used	3.2.1.9	Y | Y	
Issuer's Signature	3.2.1.11	N | Y	
Certificate Extensions		CA | EE	
Authority Key Identifier	3.2.2.1.1	N | Y	
Subject Key Identifier	3.2.2.1.2	Y | Y	
Key Usage: Digital Signature	3.2.2.1.3	N | N	Note. With most of the extensions

Requirement	Reference	Comply	Comment
KU: Non-repudiation	3.2.2.1.3	N | N	Within the NIST, they of course
KU: Key Encipherment	3.2.2.1.3	N | N	Can be set. The mechanism to
KU: Key Certificate Signature	3.2.2.1.3	N | N	Set these flags is pervasive within
KU: CRL Signature	3.2.2.1.3	N | N	The application.
Private Key Usage Period not used	3.2.2.1.4	N | N	
Certificate Policies	3.2.2.1.5	Y | Y	
Policy Mapping not used	3.2.2.1.6	Y | Y	
Subject Alternative Names	3.2.2.2.1	N | N	
Issuer Alternative Names	3.2.2.2.1	N | N	
Subject Directory Attributes not used	3.2.2.2.2	Y | Y	
Basic Constraints	3.2.2.3	Y | N	
Name Constraints	3.2.2.3	Y | Y	Neither DoD PKI or NIST requirement
Policy Constraints	3.2.2.3	Y | Y	“ “
CRL Distribution Points	3.2.2.4.1	Na | N	
Signing Algorithms		CA | EE	
RSA	3.2.3.1	N | N	
DSS	3.2.3.2	Y | Y	Signature = Sha1DSA
Certificate Types		CA | EE	
Root CA	3.2.4.1.1	P | na	
Signing CA	3.2.4.1.2	Y | na	
Identity	3.2.4.2.1	Y | Y	
E-mail	3.2.4.2.2	N | N	
Server	3.2.4.2.3	N | N	
Developer	3.2.4.2.4	N | N	
Enabled Device	3.2.4.2.5	N | N	
Certificate Revocation List (CRL) Fields		CA | EE	
Version	3.3.1.1	Y | na	
Issuer Name	3.3.1.2	Y | na	
This Update	3.3.1.3	Y | na	
Next Update	3.3.1.4	Y | na	
Revoked Certificates	3.3.1.5	Y | na	
CRL Extensions		CA | EE	
Authority Key Identifier	3.3.2.1	N | na	
Issuer Alternative Name not used	3.3.2.2	Y | na	
CRL Number	3.3.2.3	N | na	
Issuing Distribution Point	3.3.2.4	N | na	
Delta CRL Indicator	3.3.2.5	Na | na	

Requirement	Reference	Comply	Comment
CRL Entry Extensions		CA | EE	
Reason Code: Unspecified not used	3.3.3.1	Y | na	
RC: Key Compromise	3.3.3.1	Y | na	
RC: CA Compromise	3.3.3.1	Y | na	
RC: Affiliation Changed	3.3.3.1	Y | na	
RC: Superseded	3.3.3.1	Y | na	
RC: Cessation of Operations	3.3.3.1	Y | na	
RC: Certificate Hold not used	3.3.3.1	N | na	Is supported by NIST
RC: Remove from CRL	3.3.3.1	Na | na	
Expiration Date not used	3.3.3.2	Y | na	
Instruction Code not used	3.3.3.3	Y | na	
Invalidity Date	3.3.3.4	N | na	
Certificate Issuer	3.3.3.5	Y | na	
Directory Schema		CA | EE	
Directory Hierarchy	3.4.1	Y | na	
Distinguished Names	3.4.2	Y | na	
CA Directory Objects	3.4.3.1	Y | na	
Individual Directory Objects	3.4.3.2	P | na	UIN, DOB, SSN are not included in the NIST
Country Object	3.4.3.3	Y | na	
Organization Objects	3.4.3.4	Y | na	
Organizational Unit Objects	3.4.3.5	P | na	
PKI Roles Objects	3.4.3.6	N | na	
Device Objects	3.4.3.7	Na | na	
Processes		CA | EE	
Identification, Authentication and Access Control of CA Personnel	3.5.1.1	P | na	
Identification, Authentication and Access Control of RA Personnel	3.5.1.2	Y | na	
Identification, Authentication and Access Control of LRA Personnel	3.5.1.3	N | na	
Identification, Authentication and Access Control of Subscribers	3.5.1.4	Y | na	
Identity Certificate	3.5.2.1	N | na	

Requirement	Reference	Comply	Comment
Authorization, Request and Issue			
Email Certificate Authorization, Request and Issue	3.5.2.2	N | na	
Other Certificate Authorization, Request and Issue	3.5.2.3	Y | na	
Disabling Pre-Authorizations	3.5.2.4	N | na	
Processing Authorizations	3.5.2.5		
Certificate Renewal and Reissue	3.5.3	Y | na	
Certificate Expiration	3.5.4	Y | na	
Certificate Revocation	3.5.5	Y | na	
CRL Management	3.5.6	Y | na	
Certificate Removal	3.5.7	Y | na	
Key Generation	3.5.7.1	P | na	Netscape cannot request a cert
Key Recovery and Key Protection	3.5.8	N | na	
System Configuration	3.5.9.1	Y | na	
CA Management	3.5.9.2	P | na	Not via SSL
Key Management	3.5.9.3	P | na	SSL and multiple CA levels not supported
User Role Management	3.5.9.4	Y | na	
System Administrator	3.5.9.5	Y | na	
CA Staff	3.5.9.6	P | na	No SSL
RA	3.5.9.7	Y | na	
LRA	3.5.9.8	N | na	
Audit Logs	3.5.10	P | na	MS Access and Transaction logs perform this function
Archive	3.5.11	P | na	Archive does not have all fields required
Interfaces		CA | EE	
User Web Interface for Certificate Request	3.6.1.1.1	N | N	
User Web Interface for Certificate Issue	3.6.1.1.2	N | N	
User Web Interface for Directory Search	3.6.1.1.3	N | N	
System Administrator Interface	3.6.2.1	N | N	

Requirement	Reference	Comply	Comment
CA Staff Interface	3.6.2.2	N | N	
RA Interface	3.6.2.3	N | N	
LRA Interface	3.6.2.4	N | N	